Federated Authentication
Beyond The Web: Problem Statement and Requirements
http://datatracker.ietf.org/doc/draft-tschofenig-moonshot-ps/
Hannes Tschofenig
Goal: Three Party Authentication

- Challenge:
  - Scalability of relationship between IdP and RP, AND
  - Trustworthiness of information provided by IdPs
From Theory to Practice

Identity Providers (IdPs) → Federations, Trust Frameworks, Proxies… → Relying Party (RP)

User
Working Assumption: AAA

• There are many three party authentication protocols (and coming up with new approaches is not difficult).
• Challenge: Want to develop something that has the chance for widespread deployment.
• Idea: Build on top of successfully deployed infrastructures → AAA
  – Avoid modifications to AAA infrastructure
  – Keep enhancements to AAA servers small.
AAA Framework

Identity Providers (IdPs)

Proxies, Redirect Servers

Relying Party (RP)

User

Authentication Exchange E2E

Application Interaction
Working Assumption: Flexible Authentication

• The AAA infrastructure makes use of EAP. EAP offers flexible authentication by encapsulating authentication methods (called EAP methods) within EAP.

• EAP methods providing authentication support run end-to-end, from the EAP peer to the EAP server.

• EAP transport defined for RADIUS and Diameter.

• Different options for transmitting it from EAP peer to the AAA client.
  – Proposal for encapsulating EAP inside the GSS-API